

BEST AVAILABLE COPY



(19)

(11) Publication number:

11008618 A

Generated Document.

## PATENT ABSTRACTS OF JAPAN

(21) Application number: 09160039

(51) Intl. Cl.: H04L 9/32

(22) Application date: 17.06.97

(30) Priority:

(43) Date of application  
publication: 12.01.99(84) Designated contracting  
states:

(71) Applicant: TOSHIBA CORP

(72) Inventor: KATO TAKEHISA  
ENDO NAOKI

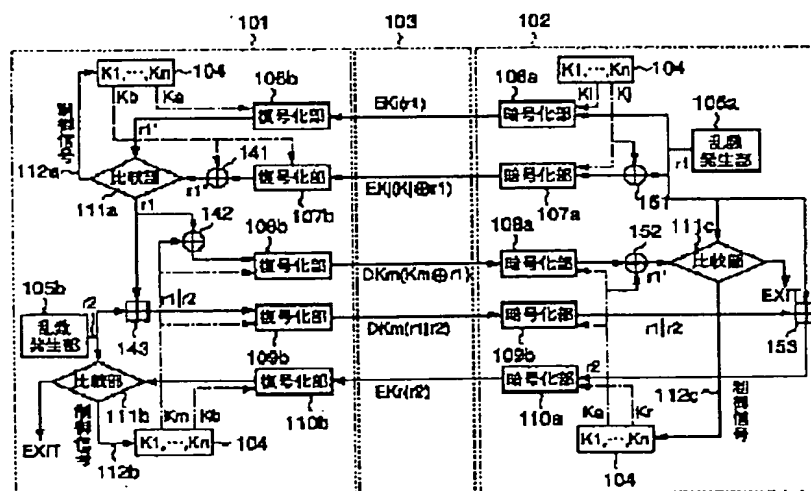
(74) Representative:

(54) DEVICE  
AUTHENTICATION METHOD,  
SYSTEM AND  
AUTHENTICATION SYSTEM

(57) Abstract:

**PROBLEM TO BE SOLVED:** To allow a system to authenticate securely and surely whether or not an opposite party is a valid device by making more difficult to estimate a secret key against a 3rd party's attack.

**SOLUTION:** The system is provided with a storage means that stores a bundle of a plurality of different private keys, a random number generating means 105a, encryption means 106a, 107a that uses a random number generated by a random number generating means or applies a prescribed arithmetic operation to the random number, uses any private key of the bundle for an encryption key to conduct encryption and to produce authentication information a communication means that sends the authentication information to a device of an authentication object, and a decoding means 108a that decodes return information received from the device of the authentication object by using the key bundle, and an authentication means 111c that compares decoding information  $r1'$  decoded by the decoding means with a random number  $r1$  and authenticates the device of the authentication object to be a legal device when the decoded information is based on the random number.



COPYRIGHT: (C)1999,JPO